JOURNAL OF COMPUTER INFORMATION SYSTEMS
Volume 55, Number 3, Spring 2015

Journal of Computer Information Systems

ISSN: 0887-4417 (Print) 2380-2057 (Online) Journal homepage: http://www.tandfonline.com/loi/ucis20

Impacts of Comprehensive Information Security Programs on Information Security Culture

Yan Chen, K. (Ram) Ramamurthy & Kuang-Wei Wen

To cite this article: Yan Chen, K. (Ram) Ramamurthy & Kuang-Wei Wen (2015) Impacts of Comprehensive Information Security Programs on Information Security Culture, Journal of Computer Information Systems, 55:3, 11-19

To link to this article: http://dx.doi.org/10.1080/08874417.2015.11645767

Published online: 10 Dec 2015.

IMPACTS OF COMPREHENSIVE INFORMATION SECURITY PROGRAMS ON INFORMATION SECURITY CULTURE

YAN CHEN
Auburn University at Montgomery
Montgomery, AL 36117

K. (RAM) RAMAMURTHY
University of Wisconsin-Milwaukee
Milwaukee, WI 53201-0742

KUANG-WEI WEN
University of Wisconsin-La Crosse
La Crosse, WI 54601

Journal of Computer Information Systems 2015.55:11-19.

ABSTRACT

A large number of security breaches involve internal employee negligence and insider breach. This situation, coupled with the need to comply with regulatory mandates has led to the establishment of comprehensive information security programs in many organizations. However, the relationships between comprehensive information security programs and security culture are unclear. This research thus proposes a research model to evaluate the influences of key components of comprehensive information security programs on security culture and empirically tests it. The results indicate that SETA programs awareness has significant influences on security culture and on employees' awareness of organizational security policy, and that the awareness of security monitoring also impacts security culture. The proposed research model can be used as a benchmark to evaluate the effectiveness of comprehensive information security programs, to improve the design of such programs should gaps exist, and eventually assist in building a security culture.

Keywords: information security culture; security policy; security monitoring; SETA programs

INTRODUCTION

Comprehensive information security programs that mainly include security policies, SETA (Security Education, Training, and Awareness) programs, and security monitoring have widely been established in many organizations to safeguard information systems (IS) and digital assets for survival and success of business. From a regulatory perspective, these comprehensive security programs are built to ensure that every employee involved in using IS becomes a part of the solution, not part of the problem, of information security [9, 32]. Security policies, SETA programs, and security monitoring as the key components of comprehensive security programs are also designed to promote organizational compliance with regulatory information security mandates such as HIPAA (Health Insurance Portability and Accountability Act), GLB (Gramm-Leach-Bliley Act), PCI DSS (Payment Card Industry Data Security Standard) and SOX (Sarbanes-Oxley Act). On the other hand, many recent studies stress the importance of establishing information security culture in organizations (e.g. [7]). These scholars suggest that one critical goal of comprehensive information security programs is to help build an information security culture in which a collection of security values, norms and knowledge are established and information security becomes a natural, inherent aspect in employees' daily information related jobs. In other words, information security culture is a collection of high level shared security values, beliefs and assumptions in information security in the organization and can lead to unconscious, continuous and habitual behaviors toward security [20, 30]. However, past literature has primarily focused on investigating the relationship between comprehensive information security programs and employees' intention to comply with the security policy [9], the impact of certain components of such programs (e.g., the effectiveness of security policy enforcement strategies on employees' security policy compliance intentions) [6], and the impact of general organizational factors such as top management support on information security culture [13]. Although more recently scholars have emphasized the important role of employees' value and belief systems, such as moral beliefs, in security policy compliance intention [8, 24] and the impact of information security culture on compliance intention [11] (literature review regarding above mentioned articles can be found in Table 1 in the Literature Review section), it is still unclear if there is any direct relationship between comprehensive information security programs[1] and the formation of information security culture in organizations. We believe establishing such direct relationship is important because culture as a strong force can reduce or diminish discrepancy in goals, enhance shared security beliefs and assumptions, and "lead to more delegation, less monitoring, higher utility (or satisfaction), higher execution effort (or motivation), less information collection, less experimentation, faster coordination, less influence activities, and less biased communication" [29, p. 1718]. We also argue that such direct relationship could (1) indicate new objectives of such programs in terms of building a security culture, and (2) establish a benchmark to evaluate the effectiveness of such programs from a socio-cultural perspective. To address this gap, our study proposes a research model to evaluate the influences of security policies, SETA programs, and security monitoring on information security culture by examining the following research questions:

1. *What are the relationships between comprehensive information security programs and information security culture?*
    a. *What is the relationship between security policies and information security culture?*
    b. *What is the relationship between SETA programs and information security culture?*
    c. *What is the relationship between security monitoring and information security culture?*
2. *What are the relationships among security policies, SETA programs, and security monitoring?*

The rest of this paper is organized as follows. In section 2, a literature review related to security policies, SETA programs, security monitoring, and information security culture is presented. Section 3 develops the research model and hypothesizes the relationship between comprehensive information security programs and information security culture. In Section 4, the research methodology and data collection are discussed. The data analysis and results are presented in Section 5. In Section 6, the results and their implications are discussed. In the final section, Section 7, limitations, future extensions of this study and contributions are discussed.

[1] *This term, which is employee-centric in this study, will be also referred to as the collection of security policies, SETA programs, and security monitoring thereafter in this paper to allow for a sharper focus on these key components.*

LITERATURE REVIEW

Comprehensive Security Programs

Comprehensive security programs are created upon the establishment of security policies through which organizations further develop a series of guidelines and procedures relating to the prevention, detection and correction cycle of information security management. Such programs need to be continuous, rather than periodic in order to ultimately change employees' mindset of security. Table 1 summarizes our literature review of comprehensive security programs as well as information security culture. First of all, s*ecurity policies* serve as internal "regulation" and "law" with an intention to foster or modify employees' favorable behaviors toward information security [9, 31]. Previous studies have found that security policies as procedural security countermeasures impacted employees' perceptions associated with security sanction [9] and formed their security policy attitudes [12]. Prior studies also have examined the impact of security enforcement policy on compliance intention [6], and the framing effect of delivering security policy [23]. However, studies have shown that employees have to be educated and trained to be aware of and be motivated to follow security policies and procedures. Otherwise, they may refuse to make needed behavioral changes or make excuses for their non-compliance behaviors [6, 24]. This is why SETA programs are recommended and introduced into organizations to enforce security policies [27, 32].

To address security policy compliance issue, *SETA programs* are being utilized to increase employees' awareness of security policies, enhance their security skills and knowledge related to their daily jobs, inform them of their responsibility for and roles in information security in the organization, and ensure their awareness of organizational sanctions and actions against security policy violation [32]. By communicating security policies, SETA programs make sure that employees understand the accountability for their behaviors toward information security. SETA programs may take different forms and get delivered at different levels [32]. SETA programs can aim at different levels of the organization from executives, senior managers, functional managers, employees, to new hires, and provide different levels of security training from general security awareness and literacy to professional development. Training materials of SETA programs could be posters, screen saving messages, videotapes, and workshops, just to list a few. Regardless of the forms and levels of SETA programs, such programs attempt to build a strong sense of security among employees so that information security becomes a natural, inherent aspect in their daily information related jobs [31]. High level of awareness of such programs is a strong indicator of the success of such programs [9]. Drawing upon the *general deterrence theory* (GDT), IS security studies also point out that SETA programs as a procedural control, particularly as a deterrence mechanism, deter IS misuse behaviors in organizations [27]. By campaigning (i.e., making it widespread within the firm) organizational sanctions and actions against security policy violation, SETA programs impact employee's perception on sanction [9].

Drawing upon and extending the GDT and following the prevention, detection and correction cycle of information security management [27], *security monitoring* records employees' usage activities of IS and collects evidence of security policy compliance or violation behaviors [11]. The main theme of the GDT is that sanctions in terms of severity and certainty of sanctions based on

TABLE 1. Summary of Literature review

Authors (Year)	Theory/ Framework	Methodology	Main Findings
Chen et al. (2013) [6]	The compliance theory and general deterrence theory	A web-based field experiment using employees recruited from Midwest companies in the US was administrated.	Both remunerative and coercive enforcement strategies as well as their interaction positively, significantly impacted employees' intention to comply with security policies. Certainty of enforcement and its interaction with both remunerative and coercive enforcement strategies also positively, significantly impacted employees' intention to comply with security policies.
Da Veiga and Eloff (2010) [7]	Information security culture framework	A survey was conducted in a South African firm.	Two security culture assessment instruments, security leadership and governance, were extracted from the framework and empirically tested. The results indicated that the framework is a valid assessment instrument on information security culture.
D'Arcy et al. (2009) [9]	The general deterrence theory	An online survey was conducted among users recruited from professionals in eight companies.	Perceived severity of sanctions had negative, significant effect on IS misuse intention, while awareness of security policies, SETA programs, and security monitoring (three major components of comprehensive security programs) had positive, significant impacts on perceived severity of sanctions. However, the proposed negative impact of perceived certainty of sanctions on IS misuse intention was not significant.
Greene and D'Arcy (2010) [11]	Moral development research models and the theory of reasoned action/planned behavior	Two surveys were conducted using an author's professional contact list.	The study proposed that security culture, job satisfaction, and perceived organizational support have a positive effect on users' compliance intention. The empirical results indicated that security culture and job satisfaction positively, significantly impact users' compliance intention, but did not support the positive relationship between perceived organizational support and users' compliance intention.
Herath and Rao (2009) [12]	The protection motivation theory and general deterrence theory	An online survey was conducted among users from 78 organizations in New York, USA.	Threat perceptions about security concern of breaches, response efficacy and self-efficacy had positive, significant impact on policy attitudes, while impact of response cost on policy attitudes was also significant but negative. In addition, self-efficacy, organizational commitment and social influence had significant, positive effect on compliance intention.

TABLE 1. Summary of Literature review cont.

Authors (Year)	Theory/ Framework	Methodology	Main Findings
Knapp et al. (2006) [13]	NA	A web-based survey was conducted among 68 CISSPs.	As proposed, the study found that top management support had significant, positive effects on an organization's security culture and level of policy enforcement.
Lee et al. (2004) [14]	The social control theory and general deterrence theory	A survey was conducted among MBA students, most with full-time jobs, at five universities in Korea.	As proposed, the study found deterrence factors, awareness of security policy and security systems had significant positive impacts on self-defense intention which in turn negatively, significantly impacted abuse by insider and outside intruders. The study also found that only two social control factors, involvement and norms, had positive, significant effects on intrusion control intention, while the proposed positive relationships between the other two social control factors, attachment and commitment, and intrusion control intention were not significant.
Schlienger and Teufel (2003) [21]	Information security culture framework	A study in a Swiss Telecom Company was conducted.	The study suggests using multiple methods, including qualitative analysis, survey, interview, and observation to study three layers of information culture in organizations. The study demoed its approach in one Swiss Telecom Company on a very conceptual level.
Siponen and Vance (2010) [24]	The neutralization theory	A survey was conducted among students and employees at one university and two companies in Finland.	Neutralization, as a formative construct with six reflective constructs including defense of necessity, appeal to higher loyalties, condemn the condemners, metaphor of the ledger, denial of injury, denial of responsibility, had positive, significant impact on intention to violate security policy.
Straub and Welke (1998) [27]	The general deterrence theory	Action research was conducted in two information services Fortune 500 firms.	The study recommended companies to use theory-based security programs including use of a security risk planning model, SETA programs, and countermeasure matrix analysis to effectively defend their information systems. In the security risk planning model, severity and certainty of sanctions, the two major, influential factors of the GDT should be emphasized.
Van Niekerk and Von Solms (2010) [30]	The organizational culture theory	Conceptual analysis	The study proposed an information security culture framework based on the organizational culture theory. The framework points out that the impacts of an information security culture on the organization's information security efforts depend on the strength of individual level and organizational level culture, and on the consistency in culture among the two levels.

the evidence of security monitoring positively impact compliance intention. Researchers and practitioners have suggested that security monitoring as a deterrence mechanism can decrease IS abuse and misuse behaviors which are subject to organizational punishment and sanction in terms of severity and certainty of sanctions [9, 27] (see Table 1 for details). Security monitoring provides review and feedback of SETA programs for continual improvement and advancement since information security is one area where organizations can never afford to stop updating [32]. In [14], the research, drawn upon the *social control theory* and the GDT, found that deterrence factors (e.g. security policy, security monitoring awareness, and security system) along with social control factors (e.g. involvement and norm) impacted computer abuse behaviors.

Comprehensive information security programs attempt to modify employees' behaviors toward information security and keep security fresh in their minds when they conduct their daily jobs. However, the underlying forces for behavioral changes are shared security attitudes, values and beliefs in the organization. Thus, there is increasing interest from researchers, practitioners, and regulators in studying and building information security culture in organizations [7, 11, 21, 30] (see Table 1 for details), as we argued above that security culture can help organizations achieve ultimate goals of security – creating security mindsets and values among employees.

Information Security Culture

Information security culture includes "all socio-cultural measures that support technical security measures" [21, p. 1]. It is viewed as an organizational sub-culture with a specific goal of information security. A large body of prior research (e.g. [19]) shows that organizational culture is an influential factor in IS adoption and diffusion (e.g. implementing enterprise systems). Following Schein's definition of organizational culture [20], information security culture is defined as a way of doing things around the information security, including creation of an environment that fosters and nurtures shared security attitudes, values and beliefs in a given organization [30]. Critical to the success of information security management in an organization, information security culture is a collection of explicit and/or implicit forces to shape employees' attitudes and behaviors towards information security in the long run. Under the influence of security culture, employees exhibit information security mindset and behaviors in a natural, taken-for granted fashion. For example, employees develop a strong security mindset of using strong passwords even though extra effort is needed. IS scholars and practitioners also believe that there is a strong link between security controls, including social and technological security controls, and security culture [7, 32]. Past studies have also pointed out that the key components of comprehensive security programs are the major part of

security controls [e.g. 7]. However, those studies have focused on theoretical frameworks of security culture and used qualitative research methods to explore the relationship between security controls and security culture (e.g. [7, 30]), leaving any possible direct association between security controls and security culture unexplored despite calls for such examination. For example, in their security culture cultivation framework, Da Veiga and Eloff [7] argued that in organizations information security components such as security policy, security program management, education and training, security monitoring and enforcement could impact security behaviors at organizational level, group level and individual level. And, in turn, security behaviors could cultivate security culture. As another example, in their three-layer security culture framework, Schlienger and Teufel [21] pointed out that security policy, implementation of security policy, training and qualification, and security monitoring and auditing can impact corporate politics, management, and individual attitudes and behaviors related to forming security culture.

From a security management perspective, prior research also examined the impact of top management support on security culture [13], and dimensions of security culture that included only one component, security monitoring, of comprehensive information security programs [11]. However, as noted, it is still unclear if there is a direct association between security controls and security culture. This link is too important to not receive more empirical attention given the vast resources and effort spent on security controls without being clear of the ensuing benefits. Finding such direct association is meaningful since trust can be put back into security programs and "the organization's mistrust against its own employees" could stop [21, p.194].

RESEARCH MODEL AND HYPOTHESES DEVELOPMENT

Research Model Development

Information security culture, as noted above, is an organizational sub-culture. Thus, we build our research model upon Schein's *organizational culture theory* [20] and Van Niekerk and Von Solms' *security culture framework* [30]; the model is shown in Figure 1. Schein [20] argued that organizational culture can manifest at three different levels—*artifacts*, *espoused values* and the ultimate, *taken-for-granted assumptions*. At the artifacts level, organizational culture can be observed through those observable objects, such as buildings, and observable behavioral patterns. Organizational culture at this level is at a surface level, and does not provide an in-depth understanding of behavioral patterns among organization members [20]. Moving to the espoused values level, organizational culture manifests itself in an organization's vision, mission, norms, and other higher level thoughts expressed in the organization's public documents, and in the mechanisms to implement and enforce those vision, mission, norms, and thoughts [20, 30]. Education, training, and awareness programs are common implementing mechanisms to build employees' awareness of the organizational vision, mission, norms, and thoughts in a format of organization's public documents. Thus, the direct intention of such programs is to move organizational culture from the surface level to the espoused values level with deeper level of thoughts and perceptions among employees [30]. The highest level of culture means that the shared, taken-for-granted assumptions are created and deeply deployed among employees [20]. Organizational culture at this level shares values and beliefs which are embedded/deeply rooted in employees' daily job-related behaviors. To reach the highest level of culture, many organizations develop and deploy comprehensive security programs. Although such programs' direct goal is to enforce the espoused culture, the ultimate goal is to create the shared, taken-for-granted assumptions [20].

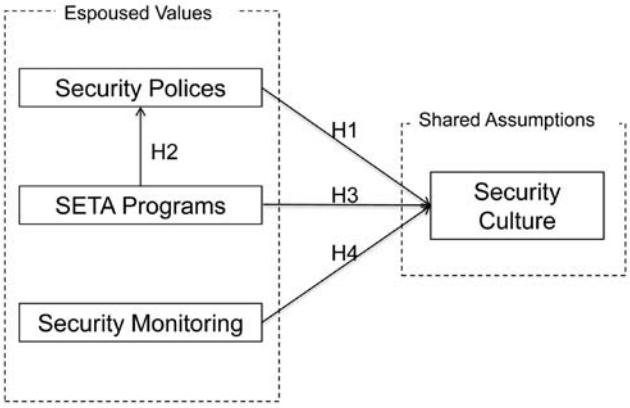

FIGURE 1. The Research Model

Drawing upon Schein's organizational culture theory [20] and Van Niekerk and Von Solms' security culture framework [30], we argue that information security culture also analogously has three levels as shown in Figure 2. Artifacts include security mechanisms that can be seen or observed, such as, computer-room locks, video surveillance systems, and authentication mechanisms. Espoused values level includes security policies, SETA programs, and security monitoring. Security policies clearly state organizational information security related vision, mission, norms, and other higher level thoughts and build a foundation to create shared values and assumptions in information security. SETA programs and security monitoring implement the control mechanisms to ensure employees' awareness of values and beliefs embodied in the security policies. In the ultimate, taken-for-granted level assumptions are the shared security thoughts and perceptions which are consistent with security values and beliefs in the organization and become strong forces to guide employees' behaviors.

We also argue that there is a relationship between espoused values of information security and the ultimate, taken-for-granted assumptions of information security. We define information security culture as a collection of high level shared security values, beliefs and assumptions in information security. Although security culture at the artifacts level is critical to information security, artifacts mainly involve physical and technical control mechanisms that are not the focus of this study for two reasons. First, such mechanisms are technically oriented, thus tangential to the socio-cultural focus of this study. Second, individuals usually react to an artifact via their perceptions and beliefs of it. Such perceptions and beliefs are formed based on their past experience

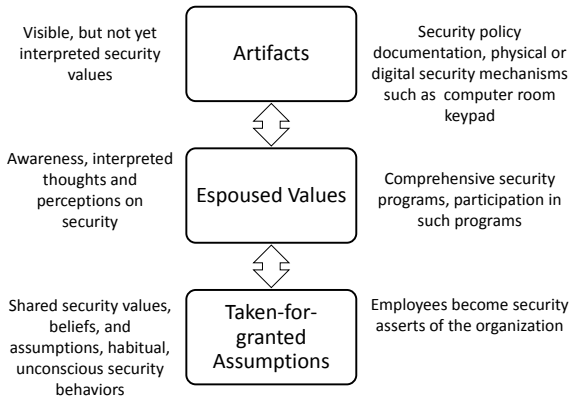

FIGURE 2. Information Security Culture Framework (adapted from [7, 21])

with a similar artifact or via organizational propaganda and training effort such as SETA programs. In other words, when interpreting security culture artifacts, individuals differ to varying degrees [25]. Thus in this study, the espoused values of security culture are captured and measured via awareness perceptions formed when employees are exposed to security culture artifacts and trained by comprehensive information security programs.

Hypotheses Development

Having formal, documented security policies in place is an initial step to shape the security culture in an organization and is even considered a best practice in the field of information security management according to regulations and industry standards (e.g. ISO (International Organization for Standardization)/ IEC (the International Electrotechnical Commission) 27001). Security policies communicate desirable attitudes and behaviors toward information security and consequences of violation of the policies by employees, and attempt to modify behaviors toward information security [6, 28]. Being aware of security policies in place indeed indicates that employees are forming deeper thoughts and perceptions on information security. Such awareness can trigger employees to internalize organizational cultural values on security. Previous studies also showed that awareness of security policies can impact employees' perceptions, attitudes and behaviors towards security [6, 9, 27]. We argue that good communication about and awareness of security policies can help to form shared values and assumptions in an organization because the organizational mission, vision and values towards information security would be better shared among employees. Thus we hypothesize,

H1. There is a positive association between employees' awareness of security polices and security culture.

SETA programs are a major means for generating and ensuring the awareness level of security policies. Beyond raising awareness, SETA programs attempt to ensure that employees interpret and understand organizational security policies as intended. As discussed in the literature review section, SETA programs also attempt to put a high value on security and, thus, to create a strong sense of security among employees [31]. In the field of social psychology, awareness programs and campaigns were found to increase norms and change attitudes towards deviant behaviors (e.g. [15]). Meanwhile, being aware of such programs and of the values of such programs can also help build a strong mindset of information security. In the IS field, the awareness of SETA programs was found to impact perceptions of sanctions for violation of security policies [9] and change attitudes [5]. Thus we argue that SETA programs deliver the organization's official viewpoints on security polices to employees, and that awareness of SETA program can increase employees' awareness level of security policies and thus to create shared values and the taken-for-granted assumptions. Following the above logic, we hypothesize that,

H2. There is a positive association between employees' awareness of SETA programs and security policies awareness.

H3. There is a positive association between employees' awareness of SETA programs and security culture.

High level security culture with ultimate, taken-for-granted values and assumptions does not get formed in the short term. It is a joint learning process among the organization and its members [30]. By collecting evidence on compliance with or violation of security policies, security monitoring exposes those unshared, misunderstood, or ignored values and assumptions relating to security and enforces the needed procedures to fix the errant aspects. By imposing punishments on violations or offering rewards for compliance, security monitoring signals moral standards and norms of security. Previous IS studies showed that employees need to be aware of security monitoring. The awareness of security monitoring can change employees' perceptions on security polices in terms of sanctions [9], because being aware of security monitoring means that employees are aware that security values are enforced in the organization. Thus we argue that security monitoring awareness can increase shared values and assumptions by providing employees with feedback on those unshared, misunderstood, or ignored values and assumptions. Following this logic, we hypothesize that,

H4. There is a positive association between employees' awareness of security monitoring and security culture.

RESEARCH METHODOLOGY

To develop the measurement scales for the constructs in the research model, an extensive literature review was conducted. The measurement indicators for employees' awareness of security policy, SETA programs, and security monitoring awareness were adapted from D'Arcy et al. 2009 [9]. The indicators used to measure security culture were adapted from Knapp et al. 2006 [13]. All measurement items were measured on 7-point scales (See Appendix A). Following recommended procedures and practices of using pilot tests to confirm instrument validity in extant literature (e.g. [26]), we conducted two pilot tests with eight information security professionals in two companies in the Midwest, USA, who were responsible for their company's information security policy development and implementation. Based on the results of the pilot tests, we modified and refined the survey. We then conducted a third pilot test with three IT professionals enrolled in an MBA class in a major university in the Midwest, and further modified and refined the survey to ensure its robustness based on the pilot test results.

A Web-based survey was used to collect data. Participants were recruited from employees in four companies in US Midwest, including the two companies where the first two pilot tests were conducted. A total of 124 participants volunteered to participate and responded to the survey. Pilot tests participants were excluded from this survey. We deleted those responses with most survey questions unanswered, leaving us with 100 usable responses.

DATA ANALYSIS AND RESULTS

We first conducted a descriptive analysis on our participants. As shown in Table 2, in terms of age 50% of the participants were younger than 35 and 49% were 35 years or older, indicating a good distribution of age in our sample. 53% had at least an undergraduate degree while 46% had an associate/professional degree or lower, also indicating a good distribution of educational background in our sample. On average, the participants had been working with their respective companies for over 7 years and within the profession for over 16 years, suggesting that they had quite a high degree of understanding of their organization and that their responses are credible.

We then conducted tests to check psychometric properties of the measures—construct validity and reliability. Following the recommendations in literature [e.g. 1, 26] that 1) factor analytic techniques are recommended to test convergent and discriminant validity, and 2) Cronbach's α, correlations, SEM composite consistency estimates are suggested to test construct reliability, we conducted the tests described below. The results shown in Table 3

TABLE 2. Demographic Characteristics of Participants

Demographic Variables	Percentage (Mean)	Std. Deviation	Min. Value	Max. Value
Gender	Males = 35%	N/A	N/A	N/A
	Females = 65%			
	Missing = 0%			
Age	18-24 years = 8%	N/A	N/A	N/A
	25-34 years = 42%			
	35-44 years = 18%			
	45-54 years = 17%			
	55-64 years = 11%			
	> 65 years = 3%			
	Missing = 1%			
Educational Background	Some School = 0%	N/A	N/A	N/A
	High School Graduate = 13%			
	Some College =17%			
	Associate/Prof. Degree = 16%			
	Undergrad Degree = 45%			
	Master's degree = 7%			
	Doctoral degree = 1%			
	Missing = 1%			
Experience within the firm (years)	(7.34)	9.44	0.0	40
Experience within the profession (years)	(16.53)	11.27	0.5	47

TABLE 3. Construct Reliability Checks

Constructs	Cronbach's α	CFR	AVE
Security Culture	.94	.94	.73
Security Policy	.79	.80	.68
SETA Program	.82	.81	.60
Security Monitoring	.90	.90	.65

show support for reliability of the various constructs in which all Cronbach's alpha values are significantly greater than the cutoff value of 0.70 [18], and all composite factor reliability (CFR) values are above the threshold of 0.70 [22]. The convergent and discriminant validity of the constructs were examined by carrying out exploratory factor analyses (EFA) by following recommendations in literature [1, 26]. In line with our expectations, four constructs emerged and all measurement items loaded on the corresponding constructs. As shown in Table 4, the Eigen values for all four extracted factors are greater than 1.0, explaining over 76% of cumulative variance, all factor loadings are greater than 0.70, and all cross loadings are less than 0.40, thus supporting the convergent and discriminant validities of the constructs [16]. The average variance extracted (AVE) values of the constructs (see Table 3) are all above the cutoff value of 0.50, further supporting the convergent validity of the constructs [10, 22]. Furthermore, as shown in Table 5, the square root of the AVE for each construct exceeds a given construct's correlations with all other three constructs, further supporting the discriminant validity of the constructs [10].

We then used the MPlus [17] software to analyze the measurement model. MPlus is a widely used statistical modeling package that offers various choices of models on latent variables, including the structural equation models for this study. All fit diagnostics, as shown in Table 6, are satisfactory: Normed χ^2 was less than the threshold value of 3.0, both CFI (Comparative Fit Index) and TLI (Tucker-Lewis Index) were greater than the recommended thresholds of 0.9, RMSEA (Root Mean Square Error of Approximation) was smaller than the threshold of 0.08, and SRMR (Standardized Root Mean Square Residual) was lower than the threshold of 0.1. Together these indices indicate a good model fit [2, 3, 4].

We also used MLM (Mean-adjusted Maximum Likelihood) in Mplus to estimate the structural model. As shown in Table 6, all fit indices were better than the threshold values recommended in extant literature [2, 3, 4], indicating a good model fit and supporting our research model. As shown in Figure 3, all the path coefficients based on the structural model estimation were statistically significant with p-values<0.05, except for the path coefficient of H1. The R^2 values of the two endogenous variables (security policies and security culture) in the research model were 0.23 and 0.37 respectively and significant at p<0.01, indicating a fairly good explanatory power of the research model.

Among the four hypotheses in the research model, three of them, H2, H3, and H4, were

TABLE 4. Extracted Factors and Factor Loadings

Indicator Items	F1: *Security Culture*	F2: *Security Policy*	F3: *SETA Program*	F4: *Security Monitoring*
Security_Culture1	**.84**	.14	.07	.18
Security_Culture2	**.87**	.08	.19	.16
Security_Culture3	**.86**	.11	.22	.11
Security_Culture4	**.87**	.15	.07	.04
Security_Culture5	**.86**	.15	.00	.22
Security_Culture6	**.75**	.27	.10	.27
Security_Policy1	.25	.09	**.75**	.10
Security_Policy2	.03	.13	**.81**	.11
Security_Policy3	.12	.17	**.85**	.12
SETA_Program1	.20	.09	.01	**.86**
SETA_Program2	.37	.07	.31	**.71**
SETA_Program3	.17	.23	.16	**.80**
Security_Monitoring1	.16	**.81**	.19	.03
Security_Monitoring2	.12	**.77**	.23	.15
Security_Monitoring3	.17	**.90**	.03	.01
Security_Monitoring4	.07	**.78**	.19	.13
Security_Monitoring5	.21	**.84**	-.10	.19
Eigen Value	6.693	2.613	1.869	1.379
Variance Explained	41.14%	15.37%	10.99%	8.11%
Cumulative Variance Explained	41.14%	56.51%	67.50%	76.61%

Journal of Computer Information Systems 2015.55:11-19.

TABLE 5. Construct Correlations and Comparison with AVEs

Constructs	1	2	3	4
1. Security Culture	**0.85**[a]			
2. Security Policy	0.33	**0.76**		
3. SETA Program	0.58	0.48	**0.77**	
4. Security Monitoring	0.38	0.18	0.370	**0.81**

[a] The square root values of the AVEs are on the diagonal.

TABLE 6. Measurement Model and DTI Model Fit Indexes

Fit Index	Measurement Model	Structural Model	Threshold*
Normed $\chi 2$	1.37	1.38	<3.0
CFI (Comparative Fit Index)	0.950	0.949	>0.90
TLI (Tucker-Lewis Index)	0.940	0.939	>0.90
RMSEA (Root Mean Square Error Of Approximation)	0.062	0.062	<0.0
SRMR (Standardized Root Mean Square Residual)	0.062	0.070	<0.10

*Based on [2, 3, 4]

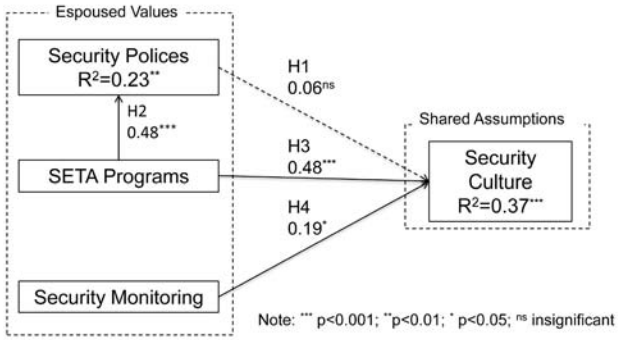

FIGURE 3. Results of Model Estimation

statistically supported (p<0.05). H2, hypothesizing the positive association between the awareness of SETA programs and the awareness of security polices in the organization, was strongly supported by the results with a high path coefficient value of 0.48 (p<0.001). H3, proposing the positive association between the awareness of the SETA programs and security culture, was also strongly supported by the results with a high path coefficient value of 0.48 (p<0.001). Both findings confirm the strong, positive associations between espoused values of the SETA programs and espoused values of security policy, and between espoused values of the SETA programs and information security culture in organizations. As hypothesized, the path between employees' awareness of security monitoring and security culture was also supported (H4), confirming that employees' espoused values of security monitoring in terms of the awareness of security monitoring has positive influence on their sense and practice of security culture within their organization. However, H1 was not supported by the results, indicating that just being aware of security policies contributes little to the organizational security culture.

DISCUSSIONS AND IMPLICATIONS

It may be recalled that a key underlying premise motivating this research was our conviction and arguments that we presented for the importance of evaluating the existence of a direct relationship between security policies, SETA programs and security monitoring to security culture because culture is a strong force that can reduce or diminish discrepancy in goals, and lead to more delegation and less monitoring, and higher efficacy of information security related investments and efforts within organizations. Drawing upon Schein's organizational culture theory [20] and the security culture framework in [30], we proposed a research model in which we hypothesized that espoused security values as manifested in employees' awareness perceptions of security policy, SETA programs, and security monitoring would have positive relationships with organizational security culture defined as the ultimate, taken-for-granted assumptions (attitudes, values and beliefs) of information security. The overall results show that our theoretical arguments for the research model are supported.

One noteworthy finding is the strong direct influence of SETA programs awareness on security culture in organizations. The implication of this finding is that it provides SETA program advocates with empirical evidence that well-designed and implemented SETA programs can change employees' perceptions, attitudes, and beliefs on information security, make them act on protecting information security even at the cost of extra effort and workload, and create an organizational security culture in which everyone assumes responsibility for information security. One other implication of this finding is that it also confirms the importance of SETA programs to include employees while formulating, designing, and developing information security policies if the intent is to build a strong and sustaining organizational security culture. Another important finding is the empirical support for the relationship between the awareness of SETA programs and security policy. Our finding is consistent with beliefs in and training practice on security in the real world [32]. As cautioned in many studies [6], human beings are usually the weakest link in achieving information security. A key implication of this finding is that merely having security policies in place without making sure that they are fully understood and favorably perceived by employees cannot instill the purpose of such policies among employees, and consequently, the effect of policies would be marginalized. Our finding clearly suggests that SETA programs are an effective means to eradicate this problem. Being aware of and understanding such programs facilitate deeper thoughts on security values and beliefs (espoused values) in security polies.

The significant path from security monitoring awareness to security culture also deserves attention. The finding shows that monitoring and assessing the compliance of security policy and practice cannot only signal employees about the organizational effort in policy enforcement, but indeed go further to influence their perceptions and assumptions on security. This finding sheds a positive new light on security monitoring. Rather than seeing employees as the worst problem of information security and using monitoring to control them, our result implies that organizations should involve employees in the development and implementation of monitoring schemes so that feedbacks on security policy compliance could help foster a positive security culture. This is a drastic departure from the general notion of security monitoring.

Interestingly, our results did not support the path from security policies awareness to security culture. One possible explanation could be that just having security policies in place does not suffice to change employees' mindset and build a security culture in organizations. An additional, perhaps more plausible, explanation might be that security policies have become so commonplace (research indicates that many organizations have at least baseline security policies in place) that employees do not consider their existence as part of a security culture. In hindsight, this finding is actually consistent with a few past studies (e.g. [6, 9]). Since security policies state organizational views and expectations on security, generally in a simple form or procedure [9], without a

proper training and enforcement strategy, the installation of these policies is "a minimalist approach to security" from employees' point of view [9, p. 92]. There apparently lies a long way between policy publishing and security culture formation. As such, our finding further underscores the importance of SETA programs and security monitoring in building security culture in organizations.

LIMITATIONS, FUTRUE STUDIES AND CONCLUSION

As with many other studies, this study has its limitations. Our sample only included employees recruited from four Midwestern companies in the United States. Caution should be taken when generalizing our findings into companies that lack comprehensive security programs. Another limitation is that there is some possibility that participants may have had a propensity to provide socially desirable answers instead of their actual thoughts in a survey approved by their managements. However, adequate cautions were taken, such as assuring anonymity of their survey responses and using neutral tone and words in the survey to reduce such a possibility. Common method bias is another limitation since we collected the data through a single study from respondents providing responses to both the antecedent and dependent variables of the model. In addition, building a security culture is a long-term process, and security culture can change over time. Our empirical study, through a single survey, could only provide a snap shot of the relationships between major security programs and security culture. To capture the dynamics of these relationships, a future longitudinal research may be necessary. And, potentially fruitful in this line of study will be identification and incorporation of additional factors such as employees' moral conduct and organizational security policy enforcement strategy impacting security culture in organizations.

In conclusion, this research makes contributions to both theory and practice. Building upon Schein's organizational culture theory [20] and the security culture framework in [30], a new research model is proposed to study the relationship between security culture and its three antecedents–employees' awareness perceptions of security policy, SETA programs, and security monitoring. For research, our findings offer significant support to the importance of SETA programs and security monitoring in building a security culture within organizations. Our novel model also offers practical implications. Information security professionals can use this model as a theoretical framework to design and assess their SETA programs. While designing SETA programs, guided by our research model, emphasis should be placed on how to change employees' perceptions, attitudes, and beliefs on security. Finally, our empirically validated model calls for a new approach to security monitoring scheme design and enforcement, which must center on employee participation and constructive feedback.

REFERENCES

[1] Anderson, J. and Gerbing, D., "Some methods for respecifying measurement models to obtain unidimensional construct measurement," *Journal of Marketing Research* (19:4), 1982, 453-460.

[2] Bentler, P.M., "On the fit of models to covariances and methodology to the bulletin," *Psychological Bulletin* (112:3), 1992, 400-404.

[3] Bentler, P.M. and Bonnett, D.G., "Significance tests and goodness of fit in the analysis of covariance structures. *Psychological Bulletin* (88:3), 1980, 588-606.

[4] Browne, M.W. and Cudeck, R., "Alternative ways of assessing model fit," *Testing Structural Equation Models,* Bollen, K.A. and Long, J.S., Eds, Newbury Park, CA: Sage, 1993, 445-455.

[5] Bulgurcu, B., Cavusoglu, H. and Benbasat, I., "Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness," *MIS Quarterly* (34:3), 2010, 523-548.

[6] Chen, Y., Ramamurthy, K. and Wen, K-W, "Organization's information security policy compliance: Stick or carrot approach?" *Journal of Management Information Systems* (29:3), 2013, 163-195.

[7] Da Veiga, A. and Eloff, J.H.P., "A framework and assessment instrument for information security culture," *Computers & Security* (29:2), 2010, 196-207.

[8] D'Arcy, J. and Herath, T., "A review and analysis of deterrence theory in the IS security literature: Making sense of the disparate findings," *European Journal of Information Systems,* (20:6), 2011, 643-658.

[9] D'Arcy, J., Hovav, A. and Galletta, D., "User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach," *Information Systems Research* (20:1), 2009, 79-98.

[10] Fornell, C. and Larcker, D.F., "Evaluating structural equation models with unobservable variables and measurement error," *Journal of Marketing Research* (18:1), 1981, 39-50.

[11] Greene, G., and D'Arcy, J, "Assessing the impact of security culture and the employee-organization relationship on IS security compliance," *Fifth Annual Symposium on Information Assurance*, Albany, NY, June 16-17, 2010.

[12] Herath, T. and Rao, H.R., "Protection motivation and deterrence: A framework for security policy compliance in organizations," *European Journal of Information Systems* (18:2), 2009, 106-125.

[13] Knapp, K.J., Marshall, T.E., Rainer, R.K. and Ford, F.N., "Information security: Management's effect on culture and policy," *Information Management & Computer Security* (14:1), 2006, 24-36.

[14] Lee, S.M., Lee, S-G, and Yoo, S., "An integrative model of computer abuse based on social control and general deterrence theories," *Information and Management* (41:6), 2004, 707-718.

[15] Mackinnon, D.P., Johnson, C.A., Pentz, M.A., Dwyer, J.H., Hansen, W.B., Flay, B.R. and Wang, E.Y., "Mediating mechanisms in a school-based drug prevention program: first-year effects of the midwestern prevention project," *Health Psychology* (10:3), 1991, 164-72.

[16] Mcknight, D.H., Choudhury, V. and Kacmar, C., "Developing and validating trust measures for e-commerce: An integrative typology," *Information Systems Research* (13:3), 2002, 334-359.

[17] Muthén, B.O. and Muthén, L., *The Comprehensive Modeling Program for Applied Researchers User Guide*, Muthén & Muthén, Los Angeles, CA, 2003.

[18] Nunnally, J., *Psychometric Theory*. McGraw-Hill, New York, 1978.

[19] Palanisamy, R., "Organizational Culture and Knowledge Management in ERP Implementation: An Empirical Study," *Journal of Computer Information Systems*, (48:2), 2007, 100-120.

[20] Schein, E.H., *The Corporate Culture Survival Guide*, San Francisco, Jossey-Bass, 1999

[21] Schlienger, T. and Teufel, S., "Analyzing information security culture: increased trust by an appropriate information security culture," 14th International Workshop on Database and Expert Systems Applications (DEXA'03), Prague, Czech Republic, 2003.

[22] Segars, A.H., "Assessing the unidimensionality of measurement: a paradigm and illustration within the context

of information systems research," *Omega* (25:1), 1997, 107-21.
[23] Shropshire, J., Warkentin, M., and Johnston, A., "Impact of Negative Message Framing On Security Adoption." *Journal of Computer Information Systems*, (51:1), 2010, 41-51.
[24] Siponen, M. and Vance, A., "Neutralization: New insights into the problem of employee systems security policy violations," *MIS Quarterly* (34:3), 2010, 487-502.
[25] Srite, M. and Karahanna, E., "The Role of Espoused National Cultural Values in Technology Acceptance," *MIS Quarterly*, (30:3), 2006, 679-704
[26] Straub, D., Boudreau, M-C and Gefen, D., "Validation guidelines for is positivist research," *Communications of the AIS* (13), 2004, 380-426.
[27] Straub, D.W. and Welke, R.J., "Coping with systems risk: Security planning models for management decision making," *MIS Quarterly* (22:4), 1998, 441-469.
[28] Thomson, K-L.N., Von Solms, R. and Louw, L., "Cultivating an organizational information security culture," *Computer Fraud & Security,* (2006:10), 2006, 7-11.
[29] Van Den Steen, E.J., "Culture clash: The costs and benefits of homogeneity," *Management Science* (56:10), 2010, 1718-1738.
[30] Van Niekerk, J.F. and Von Solms, R., "Information security culture: A management perspective," *Computers & Security* (29:4), 2010, 476-486.
[31] Whitman, M.E. "Enemy at the gate: Threats to information security," *Communications of the ACM* (46:8), 2003, 91-95.
[32] Wilson, M. and Hash, J., Building an Information Technology Security Awareness and Training Program. NIST Special Publication 800-50, National Institute of Standards and Technology, U.S. Department of Commerce, 2003.

APPENDIX A. SURVEY INSTRUMENT

Constructs	Items*
Security Culture	Employees in my organization value the importance of security of information and computer systems.
	In my organization, a culture exists that promotes good security and privacy practices.
	Security (of information and systems) has traditionally been considered an important organization value.
	Practicing good security of information and computer systems is the accepted way of doing business in my organization.
	The overall environment in my organization fosters security-minded thinking in all our actions.
	Information and systems security is a key norm shared by all organizational members/ employees.
Security Policy	My organization has established rules of behaviors for use of computer recourses.
	My organization has a formal policy that forbids employees from accessing computer systems that they are not authorized to use.
	My organization has specific guidelines that govern what employees are allowed to do with their computers.
SETA Program	In my organization, employees are briefed on the consequences of modifying computerized data in an unauthorized way.
	My organization educates employees on their computer security responsibilities.
	In my organization, employees are briefed on the consequences of accessing computer systems that they are not authorized to use.
Security Monitoring	I believe that employee computing activities are monitored by my organization.
	I believe that my organization monitors computing activities to ensure that employees are performing only explicitly authorized tasks.
	I believe that my organization reviews logs of employee computing activities on a regular basis
	I believe that my organization conducts periodic audits to detect the use of authorized software on its computers.
	I believe that my organization actively monitors the content of employees' e-mail messages.

*: we use 7-point scales: 1=strongly disagree, 7= strongly agree

Journal of Computer Information Systems 2015.55:11-19.